CLAIMS

1. A signal process system having a record and reproduction apparatus that reads information from a record medium and records information thereto, and an information process apparatus to which the record and reproduction apparatus is connected through transfer means, content information being encrypted according to a content information encryption method using a first encrypted key managed by a management mechanism, a second encrypted key unique to the record medium, and a third encrypted key generated whenever information is recorded, the content information being recorded to the record medium,

wherein the record and reproduction apparatus comprises:

storage means for storing the first encrypted key,

second encrypted key decryption means for reproducing the second encrypted key encrypted and recorded on the record medium and for decrypting the second encrypted key with the first encrypted key,

third encrypted key generation means for generating the third encrypted key,

encryption means for encrypting the third encrypted key with the decrypted second encrypted key,

authentication means for authenticating the information process apparatus and generating a session

key when the authentication means has successfully authenticated the information process apparatus,

first bus-encryption means for bus-encrypting the second encrypted key that has been encrypted and recorded on the record medium with the session key and transferring the bus-encrypted second encrypted key to the information process apparatus,

second bus-encryption means for bus-encrypting the third encrypted key with the session key and transferring the bus-encrypted third encrypted key to the information process apparatus,

bus-decryption means for bus-decrypting encrypted and bus-encrypted content information supplied from the information process apparatus, and

record means for recording the third encrypted key and the encrypted content information to the record medium, and

wherein the information process apparatus comprises:

storage means for storing the first encrypted key,

authentication means for authenticating the record and reproduction apparatus and generating the session key when the authentication means has successfully authenticated the record and reproduction apparatus,

first bus-decryption means for bus-decrypting

the bus-encrypted second encrypted key with the session key,

decryption means for decrypting the second encrypted key with the first encrypted key,

second bus-decryption means for bus-decrypting the bus-encrypted third encrypted key with the session key,

decryption means for decrypting the third encrypted key with the second encrypted key,

encryption means for encrypting the content information transferred to the record and reproduction apparatus with the third encryption, and

bus-encryption means for bus-encrypting the encrypted content information with the session key and sending the bus-encrypted content information to the record and reproduction apparatus.

2. The signal process system as set forth in claim 1,

wherein the authentication means of the record and reproduction apparatus and the authentication means of the information process apparatus mix a random number transferred from the record and reproduction apparatus to the information process apparatus with information about a type of the record medium when the authentication means of the record and reproduction apparatus and the authentication means of the information process

apparatus exchange the generated random number data therebetween.

3. The signal process system as set forth in claim 1,

wherein the authentication means of the record and reproduction apparatus and the authentication means of the information process apparatus mix a random number transferred from the record and reproduction apparatus to the information process apparatus with information about copyright when the authentication means of the record and reproduction apparatus and the authentication means of the information process apparatus exchange the generated random number data therebetween.

4. The signal process system as set forth in claim 1, further comprising:

mask control means for the third encrypted key,

wherein only when the authentication means of the record and reproduction apparatus and the authentication means of the information process apparatus have mutually and successfully authenticated each other, the third encrypted key can be written to the record medium.

5. A signal process system having a record and reproduction apparatus that reads information from a record medium and records information thereto, and an

information process apparatus to which the record and reproduction apparatus is connected through transfer means, content information being encrypted according to a content information encryption method using a first encrypted key managed by a management mechanism, a second encrypted key unique to the record medium, and a third encrypted key generated whenever information is recorded, the content information being recorded to the record medium, wherein the record and reproduction apparatus comprises:

storage means for storing the first encrypted key,

second encrypted key generation means for generating the second encrypted key,

encryption means for encrypting the generated second encrypted key with the first encrypted key,

third encrypted key generation means for generating the third encrypted key,

encryption means for encrypting the third encrypted key with the generated second encrypted key,

authentication means for authenticating the information process apparatus and generating a session key when the authentication means has successfully authenticated the information process apparatus,

first bus-encryption means for bus-encrypting the second encrypted key with the session key and transferring the bus-encrypted second encrypted key to

the information process apparatus,

second bus-encryption means for bus-encrypting the third encrypted key with the session key and transferring the bus-encrypted third encrypted key to the information process apparatus,

bus-decryption means for bus-decrypting the encrypted and bus-encrypted content information supplied from the information process apparatus, and

record means for recording the second encrypted key, the third encrypted key, and the encrypted content information to the record medium, and

wherein the information process apparatus comprises:

storage means for storing the first encrypted key,

authentication means for authenticating the record and reproduction apparatus and generating the session key when the authentication means has successfully authenticated the record and reproduction apparatus,

first bus-decryption means for bus-decrypting the bus-encrypted second encrypted key with the session key,

decryption means for decrypting the second encrypted key with the first encrypted key,

second bus-decryption means for bus-decrypting the bus-encrypted third encrypted key with

the session key,

decryption means for decrypting the third encrypted key with the second encrypted key,

encryption means for encrypting the content information transferred to the record and reproduction apparatus with the third encryption, and

bus-encryption means for bus-encrypting the encrypted content information with the session key and sending the bus-encrypted content information to the record and reproduction apparatus.

6. The signal process system as set forth in claim 5,

wherein the authentication means of the record and reproduction apparatus and the authentication means of the information process apparatus mix a random number transferred from the record and reproduction apparatus to the information process apparatus with information about a type of the record medium when the authentication means of the record and reproduction apparatus and the authentication means of the information process apparatus exchange the generated random number data therebetween.

7. The signal process system as set forth in claim 5,

wherein the authentication means of the record and reproduction apparatus and the

authentication means of the information process apparatus mix a random number transferred from the record and reproduction apparatus to the information process apparatus with information about copyright when the authentication means of the record and reproduction apparatus and the authentication means of the information process apparatus exchange the generated random number data therebetween.

8. The signal process system as set forth in claim 5, further comprising:

first mask control means for the third encrypted key, and

second mask control means for the second encrypted key,

wherein only when the authentication means of the record and reproduction apparatus and the authentication means of the information process apparatus have mutually and successfully authenticated each other, the third encrypted key and the second encrypted key can be written to the record medium.

9. A signal process system having a record and reproduction apparatus that reads information from a record medium and records information thereto, and an information process apparatus to which the record and reproduction apparatus is connected through transfer means, content information being encrypted according to a content information encryption method using a first

encrypted key managed by a management mechanism, a second encrypted key unique to the record medium, and a third encrypted key generated whenever information is recorded, the content information being recorded to the record medium,

wherein the record and reproduction apparatus comprises:

storage means for storing the first encrypted key,

second encrypted key decryption means for reproducing the second encrypted key encrypted and recorded on the record medium and for decrypting the second encrypted key with the first encrypted key,

third encrypted key generation means for generating the third encrypted key,

encryption means for encrypting the third encrypted key with the decrypted second encrypted key,

authentication means for authenticating the information process apparatus and generating a session key when the authentication means has successfully authenticated the information process apparatus,

bus-decryption means for bus-decrypting the bus-encrypted content information supplied from the information process apparatus,

encryption means for encrypting the content information with the third encrypted key, and

record means for recording the third

encrypted key and the encrypted content information to the record medium, and

wherein the information process apparatus comprises:

authentication means for authenticating the record and reproduction apparatus and generating the session key when the information process apparatus has successfully authenticated the record and reproduction apparatus, and

bus-encryption means for bus-encrypting content information transferred to the record and reproduction apparatus with the session key and sending the bus-encrypted content information to the record and reproduction apparatus.

10. The signal process system as set forth in claim 9,

wherein the authentication means of the record and reproduction apparatus and the authentication means of the information process apparatus mix a random number transferred from the record and reproduction apparatus to the information process apparatus with information about a type of the record medium when the authentication means of the record and reproduction apparatus and the authentication means of the information process apparatus exchange the generated random number data therebetween.

11. The signal process system as set forth in claim 9,

wherein the authentication means of the record and reproduction apparatus and the authentication means of the information process apparatus mix a random number transferred from the record and reproduction apparatus to the information process apparatus with information about copyright when the authentication means of the record and reproduction apparatus and the authentication means of the information process apparatus exchange the generated random number data therebetween.

12. The signal process system as set forth in claim 9, further comprising:

mask control means for the third encrypted key,

wherein only when the authentication means of the record and reproduction apparatus and the authentication means of the information process apparatus have mutually and successfully authenticated each other, the third encrypted key can be written to the record medium.

13. A signal process system having a record and reproduction apparatus that reads information from a record medium and records information thereto, and an information process apparatus to which the record and reproduction apparatus is connected through transfer

means, content information being encrypted according to a content information encryption method using a first encrypted key managed by a management mechanism, a second encrypted key unique to the record medium, and a third encrypted key generated whenever information is recorded, the content information being recorded to the record medium,

wherein the record and reproduction apparatus comprises:

storage means for storing the first encrypted key,

second encrypted key generation means for generating the second encrypted key,

encryption means for encrypting the generated second encrypted key with the first encrypted key,

third encrypted key generation means for generating the third encrypted key,

encryption means for encrypting the third encrypted key with the generated second encrypted key,

authentication means for authenticating the information process apparatus and generating a session key when the authentication means has successfully authenticated the information process apparatus,

bus-decryption means for bus-decrypting the bus-encrypted content information supplied from the information process apparatus,

encryption means for encrypting the content

information with the third encrypted key, and

record means for recording the second encrypted key, the third encrypted key, and the encrypted content information to the record medium, and

wherein the information process apparatus comprises:

authentication means for authenticating the record and reproduction apparatus and generating the session key when the information process apparatus has successfully authenticated the record and reproduction apparatus, and

bus-encryption means for bus-encrypting content information with the session key and sending the bus-encrypted content information to the record and reproduction apparatus.

14. The signal process system as set forth in claim 13,

wherein the authentication means of the record and reproduction apparatus and the authentication means of the information process apparatus mix a random number transferred from the record and reproduction apparatus to the information process apparatus with information about a type of the record medium when the authentication means of the record and reproduction apparatus and the authentication means of the information process apparatus exchange the generated random number data

therebetween.

15. The signal process system as set forth in claim 13,

wherein the authentication means of the record and reproduction apparatus and the authentication means of the information process apparatus mix a random number transferred from the record and reproduction apparatus to the information process apparatus with information about copyright when the authentication means of the record and reproduction apparatus and the authentication means of the information process apparatus exchange the generated random number data therebetween.

16. The signal process system as set forth in claim 13, further comprising:

first mask control means for the third encrypted key, and

second mask control means for the second encrypted key,

wherein only when the authentication means of the record and reproduction apparatus and the authentication means of the information process apparatus have mutually and successfully authenticated each other, the third encrypted key and the second encrypted key can be written to the record medium.

17. A record and reproduction apparatus that is connected to an information process apparatus through

transfer means and that reads information from a record medium and records information thereto, content information being encrypted according to a content information encryption method using a first encrypted key managed by a management mechanism, a second encrypted key unique to the record medium, and a third encrypted key generated whenever information is recorded, the content information being recorded to the record medium, the record and reproduction apparatus comprising:

storage means for storing the first encrypted key,

second encrypted key decryption means for reproducing the second encrypted key encrypted and recorded on the record medium and for decrypting the second encrypted key with the first encrypted key,

third encrypted key generation means for generating the third encrypted key,

encryption means for encrypting the third encrypted key with the decrypted second encrypted key,

authentication means for authenticating the information process apparatus and generating a session key when the authentication means has successfully authenticated the information process apparatus,

first bus-encryption means for bus-encrypting the second encrypted key that has been encrypted and recorded on the record medium with the session key and

transferring the bus-encrypted second encrypted key to the information process apparatus,

second bus-encryption means for bus-encrypting the third encrypted key with the session key and transferring the bus-encrypted third encrypted key to the information process apparatus,

bus-decryption means for bus-decrypting encrypted and bus-encrypted content information supplied from the information process apparatus,

record means for recording the third encrypted key and the encrypted content information to the record medium,

wherein the encrypted and bus-encrypted content information is encrypted with the third encrypted key and the encrypted content information is bus-encrypted with the session key generated by the information process apparatus.

18. The record and reproduction apparatus as set forth in claim 17,

wherein the authentication means mixes a random number transferred to the information process apparatus with information about a type of the record medium when the authentication means exchanges random number data with the information process apparatus.

19. The record and reproduction apparatus as set forth in claim 17, further comprising:

mask control means for the third encrypted

key,

wherein only when the authentication means has successfully authenticated the information process apparatus, the third encrypted key can be written to the record medium.

20. A record and reproduction apparatus that is connected to an information process apparatus through transfer means and that reads information from a record medium and records information thereto, content information being encrypted according to a content information encryption method using a first encrypted key managed by a management mechanism, a second encrypted key unique to the record medium, and a third encrypted key generated whenever information is recorded, the content information being recorded to the record medium, the record and reproduction apparatus comprising:

storage means for storing the first encrypted key,

second encrypted key generation means for generating the second encrypted key,

encryption means for encrypting the generated second encrypted key with the first encrypted key,

third encrypted key generation means for generating the third encrypted key,

encryption means for encrypting the third encrypted key with the generated second encrypted key,

authentication means for authenticating the information process apparatus and generating a session key when the authentication means has successfully authenticated the information process apparatus,

first bus-encryption means for bus-encrypting the second encrypted key with the session key and transferring the bus-encrypted second encrypted key to the information process apparatus,

second bus-encryption means for bus-encrypting the third encrypted key with the session key and transferring the bus-encrypted third encrypted key to the information process apparatus,

bus-decryption means for bus-decrypting the encrypted and bus-encrypted content information supplied from the information process apparatus, and

record means for recording the second encrypted key, the third encrypted key, and the encrypted content information to the record medium,

wherein the encrypted and bus-encrypted content information is encrypted with the third encrypted key and the encrypted content information is bus-encrypted with the session key generated by the information process apparatus.

21. The record and reproduction apparatus as set forth in claim 20,

wherein the authentication means mixes a random number transferred to the information process

apparatus with information about a type of the record medium when the authentication means exchanges random number data with the information process apparatus.

22. The record and reproduction apparatus as set forth in claim 20, further comprising:

first mask control means for the third encrypted key, and

second mask control means for the second encrypted key,

wherein only when the authentication means has successfully authenticated the information process apparatus, the third encrypted key and the second encrypted key can be written to the record medium.

23. A record and reproduction apparatus that is connected to an information process apparatus through transfer means and that reads information from a record medium and records information thereto, content information being encrypted according to a content information encryption method using a first encrypted key managed by a management mechanism, a second encrypted key unique to the record medium, and a third encrypted key generated whenever information is recorded, the content information being recorded to the record medium, the record and reproduction apparatus comprising:

storage means for storing the first encrypted key,

second encrypted key decryption means for reproducing the second encrypted key encrypted and recorded to the record medium and for decrypting the second encrypted key with the first encrypted key,

third encrypted key generation means for generating the third encrypted key,

encryption means for encrypting the third encrypted key with the decrypted second encrypted key,

authentication means for authenticating the information process apparatus and generating a session key when the authentication means has successfully authenticated the information process apparatus,

bus-decryption means for bus-decrypting the bus-encrypted content information supplied from the information process apparatus,

encryption means for encrypting the content information with the third encrypted key, and

record means for recording the third encrypted key and the encrypted content information to the record medium,

wherein the bus-encrypted content information is the encrypted content information that has been bus-encrypted with the session key generated by the information process apparatus.

24. The record and reproduction apparatus as set forth in claim 23,

wherein the authentication means mixes a

random number transferred to the information process apparatus with information about a type of the record medium when the authentication means exchanges random number data with the information process apparatus.

25. The record and reproduction apparatus as set forth in claim 23, further comprising:

mask control means for the third encrypted key,

wherein only when the authentication means has successfully authenticated the information process apparatus, the third encrypted key can be written to the record medium.

26. A record and reproduction apparatus that is connected to an information process apparatus through transfer means and that reads information from a record medium and records information thereto, content information being encrypted according to a content information encryption method using a first encrypted key managed by a management mechanism, a second encrypted key unique to the record medium, and a third encrypted key generated whenever information is recorded, the content information being recorded to the record medium, the record and reproduction apparatus comprising:

storage means for storing the first encrypted key,

second encrypted key generation means for

generating the second encrypted key,

encryption means for encrypting the generated second encrypted key with the first encrypted key,

third encrypted key generation means for generating the third encrypted key,

encryption means for encrypting the third encrypted key with the generated second encrypted key,

authentication means for authenticating the information process apparatus and generating a session key when the authentication means has successfully authenticated the information process apparatus,

bus-decryption means for bus-decrypting the bus-encrypted content information supplied from the information process apparatus,

encryption means for encrypting the content information with the third encrypted key, and

record means for recording the second encrypted key, the third encrypted key, and the encrypted content information to the record medium,

wherein the bus-encrypted content information is the encrypted content information that has been bus-encrypted with the session key generated by the information process apparatus.

27. The record and reproduction apparatus as set forth in claim 26,

wherein the authentication means mixes a random number transferred to the information process

apparatus with information about a type of the record medium when the authentication means exchanges random number data with the information process apparatus.

28. The record and reproduction apparatus as set forth in claim 26, further comprising:

first mask control means for the third encrypted key, and

second mask control means for the second encrypted key,

wherein only when the authentication means has successfully authenticated the information process apparatus, the third encrypted key and the second encrypted key can be written to the record medium.

29. A record method of a record and reproduction apparatus that reads information from a record medium and records information thereto and an information process apparatus to which the record and reproduction apparatus is connected through transfer step, content information being encrypted according to a content information encryption method using a first encrypted key managed by a management mechanism, a second encrypted key unique to the record medium, and a third encrypted key generated whenever information is recorded, the content information being recorded to the record medium, the record method comprising the steps of:

causing the record and reproduction apparatus

to store the first encrypted key,

causing the record and reproduction apparatus to reproduce the second encrypted key encrypted and recorded on the record medium and decrypt the second encrypted key with the first encrypted key,

causing the record and reproduction apparatus to generate the third encrypted key,

causing the record and reproduction apparatus to encrypt the third encrypted key with the decrypted second encrypted key,

causing the record and reproduction apparatus to authenticate the information process apparatus and generate a session key when the record and reproduction apparatus has successfully authenticated the information process apparatus ,

causing the record and reproduction apparatus to bus-encrypt the second encrypted key that has been encrypted and recorded on the record medium with the session key and transfer the bus-encrypted second encrypted key to the information process apparatus,

causing the record and reproduction apparatus to bus-encrypt the third encrypted key with the session key and transfer the bus-encrypted third encrypted key to the information process apparatus,

causing the record and reproduction apparatus to bus-decrypt the encrypted and bus-encrypted content information supplied from the information process

apparatus,

causing the record and reproduction apparatus to record the third encrypted key and the encrypted content information to the record medium,

causing the information process apparatus to store the first encrypted key,

causing the information process apparatus to authenticate the record and reproduction apparatus and generate the session key when the information process apparatus has successfully authenticated the record and reproduction apparatus,

causing the information process apparatus to bus-decrypt the bus-encrypted second encrypted key with the session key,

causing the information process apparatus to decrypt the second encrypted key with the first encrypted key,

causing the information process apparatus to bus-decrypt the bus-encrypted third encrypted key with the session key,

causing the information process apparatus to decrypt the third encrypted key with the second encrypted key,

causing the information process apparatus to encrypt the content information transferred to the record and reproduction apparatus with the third encryption, and

causing the information process apparatus to bus-encrypt the encrypted content information with the session key and send the bus-encrypted content information to the record and reproduction apparatus.

30. The record method as set forth in claim 29, wherein at the authentication step of the record and reproduction apparatus and the authentication step of the information process apparatus, a random number transferred from the record and reproduction apparatus to the information process apparatus is mixed with information about a type of the record medium when the generated random number data are exchanged therebetween.

31. The record method as set forth in claim 29, wherein at the authentication step of the record and reproduction apparatus and the authentication step of the information process apparatus, a random number transferred from the record and reproduction apparatus to the information process apparatus is mixed with information about copyright when the generated random number data are exchanged therebetween.

32. The record method as set forth in claim 29, further comprising the step of:

mask-controlling the third encrypted key, wherein only when at the authentication step of the record and reproduction apparatus and the

authentication step of the information process apparatus, they have been mutually and successfully authenticated each other, the third encrypted key can be written to the record medium.

33. A record method of a record and reproduction apparatus that reads information from a record medium and records information thereto and an information process apparatus to which the record and reproduction apparatus is connected through transfer step, content information being encrypted according to a content information encryption method using a first encrypted key managed by a management mechanism, a second encrypted key unique to the record medium, and a third encrypted key generated whenever information is recorded, the content information being recorded to the record medium, the record method comprising the steps of:

causing the record and reproduction apparatus to store the first encrypted key,

causing the record and reproduction apparatus to generate the second encrypted key,

causing the record and reproduction apparatus to encrypt the generated second encrypted key with the first encrypted key,

causing the record and reproduction apparatus to generate the third encrypted key,

causing the record and reproduction apparatus

to encrypt the third encrypted key with the generated second encrypted key,

causing the record and reproduction apparatus to authenticate the information process apparatus and generate a session key when the record and reproduction apparatus has successfully authenticated the information process apparatus,

causing the record and reproduction apparatus to bus-encrypt the second encrypted key with the session key and transfers the bus-encrypted second encrypted key to the information process apparatus,

causing the record and reproduction apparatus to bus-encrypt the third encrypted key with the session key and transfer the bus-encrypted third encrypted key to the information process apparatus,

causing the record and reproduction apparatus to bus-decrypt the encrypted and bus-encrypted content information supplied from the information process apparatus, and

causing the record and reproduction apparatus to record the second encrypted key, the third encrypted key, and the encrypted content information to the record medium, and

causing the information process apparatus to store the first encrypted key,

causing the information process apparatus to authenticate the record and reproduction apparatus and

generate the session key when the information process apparatus has successfully authenticated the record and reproduction apparatus,

causing the information process apparatus to bus-decrypt the bus-encrypted second encrypted key with the session key,

causing the information process apparatus to decrypt the second encrypted key with the first encrypted key,

causing the information process apparatus to bus-decrypt the bus-encrypted third encrypted key with the session key,

causing the information process apparatus to decrypt the third encrypted key with the second encrypted key,

causing the information process apparatus to encrypt the content information transferred to the record and reproduction apparatus with the third encryption, and

causing the information process apparatus to bus-encrypt the encrypted content information with the session key and send the bus-encrypted content information to the record and reproduction apparatus.

34. The record method as set forth in claim 33,

wherein at the authentication step of the record and reproduction apparatus and the authentication step of the information process

apparatus, a random number transferred from the record and reproduction apparatus to the information process apparatus is mixed with information about a type of the record medium when the generated random number data are exchanged therebetween.

35. The record method as set forth in claim 33, wherein at the authentication step of the record and reproduction apparatus and the authentication step of the information process apparatus, a random number transferred from the record and reproduction apparatus to the information process apparatus is mixed with information about copyright when the generated random number data are exchanged therebetween.

36. The record method as set forth in claim 33, further comprising the steps of:

mask-controlling the third encrypted key, and

mask-controlling the second encrypted key,

wherein only when at the authentication step of the record and reproduction apparatus and the authentication step of the information process apparatus, they have been mutually and successfully authenticated each other, the third encrypted key and the second encrypted key can be written to the record medium.

37. A record method of a record and reproduction apparatus that reads information from a record medium

and records information thereto and an information process apparatus to which the record and reproduction apparatus is connected through transfer step, content information being encrypted according to a content information encryption method using a first encrypted key managed by a management mechanism, a second encrypted key unique to the record medium, and a third encrypted key generated whenever information is recorded, the content information being recorded to the record medium, the record method comprising the steps of:

causing the record and reproduction apparatus to store the first encrypted key,

causing the record and reproduction apparatus to reproduce the second encrypted key encrypted and recorded on the record medium and decrypt the second encrypted key with the first encrypted key,

causing the record and reproduction apparatus to generate the third encrypted key,

causing the record and reproduction apparatus to encrypt the third encrypted key with the decrypted second encrypted key,

causing the record and reproduction apparatus to authenticate the information process apparatus and generate a session key when the record and reproduction apparatus has successfully authenticated the information process apparatus,

causing the record and reproduction apparatus to bus-decrypt the bus-encrypted content information supplied from the information process apparatus,

causing the record and reproduction apparatus to encrypt the content information with the third encrypted key,

causing the record and reproduction apparatus to record the third encrypted key and the encrypted content information to the record medium, and

causing the information process apparatus to authenticate the record and reproduction apparatus and generate the session key when the information process apparatus has successfully authenticated the record and reproduction apparatus, and

causing the information process apparatus to bus-encrypt content information transferred to the record and reproduction apparatus with the session key and send the bus-encrypted content information to the record and reproduction apparatus.

38. The record method as set forth in claim 37,

wherein at the authentication step of the record and reproduction apparatus and the authentication step of the information process apparatus, a random number transferred from the record and reproduction apparatus to the information process apparatus is mixed with information about a type of the record medium when the generated random number data are

exchanged therebetween.

39. The record method as set forth in claim 37, wherein at the authentication step of the record and reproduction apparatus and the authentication step of the information process apparatus, a random number transferred from the record and reproduction apparatus to the information process apparatus is mixed with information about copyright when the generated random number data are exchanged therebetween.

40. The record method as set forth in claim 37, further comprising the step of:

mask-controlling the third encrypted key, wherein only when at the authentication step of the record and reproduction apparatus and the authentication step of the information process apparatus, they have been mutually and successfully authenticated each other, the third encrypted key can be written to the record medium.

41. A record method of a record and reproduction apparatus that reads information from a record medium and records information thereto and an information process apparatus to which the record and reproduction apparatus is connected through transfer step, content information being encrypted according to a content information encryption method using a first encrypted key managed by a management mechanism, a second

encrypted key unique to the record medium, and a third encrypted key generated whenever information is recorded, the content information being recorded to the record medium, the record method comprising the steps of:

causing the record and reproduction apparatus to store the first encrypted key,

causing the record and reproduction apparatus to generate the second encrypted key,

causing the record and reproduction apparatus to encrypt the generated second encrypted key with the first encrypted key,

causing the record and reproduction apparatus to generate the third encrypted key,

causing the record and reproduction apparatus to encrypt the third encrypted key with the generated second encrypted key,

causing the record and reproduction apparatus to authenticate the information process apparatus and generate a session key when the record and reproduction apparatus has successfully authenticated the information process apparatus,

causing the record and reproduction apparatus to bus-decrypt the bus-encrypted content information supplied from the information process apparatus,

causing the record and reproduction apparatus to encrypt the content information with the third

encrypted key,

causing the record and reproduction apparatus to record the second encrypted key, the third encrypted key, and the encrypted content information to the record medium,

causing the information process apparatus to authenticate the record and reproduction apparatus and generate the session key when the information process apparatus has successfully authenticated the record and reproduction apparatus, and

causing the information process apparatus to bus-encrypt content information with the session key and send the bus-encrypted content information to the record and reproduction apparatus.

42. The record method as set forth in claim 41,

wherein at the authentication step of the record and reproduction apparatus and the authentication step of the information process apparatus, a random number transferred from the record and reproduction apparatus to the information process apparatus is mixed with information about a type of the record medium when the generated random number data are exchanged therebetween.

43. The record method as set forth in claim 41,

wherein at the authentication step of the record and reproduction apparatus and the authentication step of the information process

apparatus, a random number transferred from the record and reproduction apparatus to the information process apparatus is mixed with information about copyright when the generated random number data are exchanged therebetween.

44. The record method as set forth in claim 41, further comprising the steps of:

mask-controlling the third encrypted key, and

mask-controlling the second encrypted key,

wherein only when at the authentication step of the record and reproduction apparatus and the authentication step of the information process apparatus, they have been mutually and successfully authenticated each other, the third encrypted key and the second encrypted key can be written to the record medium.

45. A program of a record method of a record and reproduction apparatus that reads information from a record medium and records information thereto and an information process apparatus to which the record and reproduction apparatus is connected through transfer step, content information being encrypted according to a content information encryption method using a first encrypted key managed by a management mechanism, a second encrypted key unique to the record medium, and a third encrypted key generated whenever information is recorded, the content information being recorded to the

record medium, the record method comprising the steps of:

causing the record and reproduction apparatus to store the first encrypted key,

causing the record and reproduction apparatus to reproduce the second encrypted key encrypted and recorded on the record medium and decrypt the second encrypted key with the first encrypted key,

causing the record and reproduction apparatus to generate the third encrypted key,

causing the record and reproduction apparatus to encrypt the third encrypted key with the decrypted second encrypted key,

causing the record and reproduction apparatus to authenticate the information process apparatus and generate a session key when the record and reproduction apparatus has successfully authenticated the information process apparatus ,

causing the record and reproduction apparatus to bus-encrypt the second encrypted key that has been encrypted and recorded on the record medium with the session key and transfer the bus-encrypted second encrypted key to the information process apparatus,

causing the record and reproduction apparatus to bus-encrypt the third encrypted key with the session key and transfer the bus-encrypted third encrypted key to the information process apparatus,

causing the record and reproduction apparatus to bus-decrypt the encrypted and bus-encrypted content information supplied from the information process apparatus,

causing the record and reproduction apparatus to record the third encrypted key and the encrypted content information to the record medium,

causing the information process apparatus to store the first encrypted key,

causing the information process apparatus to authenticate the record and reproduction apparatus and generate the session key when the information process apparatus has successfully authenticated the record and reproduction apparatus,

causing the information process apparatus to bus-decrypt the bus-encrypted second encrypted key with the session key,

causing the information process apparatus to decrypt the second encrypted key with the first encrypted key,

causing the information process apparatus to bus-decrypt the bus-encrypted third encrypted key with the session key,

causing the information process apparatus to decrypt the third encrypted key with the second encrypted key,

causing the information process apparatus to

encrypt the content information transferred to the record and reproduction apparatus with the third encryption, and

causing the information process apparatus to bus-encrypt the encrypted content information with the session key and send the bus-encrypted content information to the record and reproduction apparatus.

46. A program of a record method of a record and reproduction apparatus that reads information from a record medium and records information thereto and an information process apparatus to which the record and reproduction apparatus is connected through transfer step, content information being encrypted according to a content information encryption method using a first encrypted key managed by a management mechanism, a second encrypted key unique to the record medium, and a third encrypted key generated whenever information is recorded, the content information being recorded to the record medium, the record method comprising the steps of:

causing the record and reproduction apparatus to store the first encrypted key,

causing the record and reproduction apparatus to generate the second encrypted key,

causing the record and reproduction apparatus to encrypt the generated second encrypted key with the first encrypted key,

causing the record and reproduction apparatus to generate the third encrypted key,

causing the record and reproduction apparatus to encrypt the third encrypted key with the generated second encrypted key,

causing the record and reproduction apparatus to authenticate the information process apparatus and generate a session key when the record and reproduction apparatus has successfully authenticated the information process apparatus,

causing the record and reproduction apparatus to bus-encrypt the second encrypted key with the session key and transfers the bus-encrypted second encrypted key to the information process apparatus,

causing the record and reproduction apparatus to bus-encrypt the third encrypted key with the session key and transfer the bus-encrypted third encrypted key to the information process apparatus,

causing the record and reproduction apparatus to bus-decrypt the encrypted and bus-encrypted content information supplied from the information process apparatus, and

causing the record and reproduction apparatus to record the second encrypted key, the third encrypted key, and the encrypted content information to the record medium, and

causing the information process apparatus to

store the first encrypted key,

causing the information process apparatus to authenticate the record and reproduction apparatus and generate the session key when the information process apparatus has successfully authenticated the record and reproduction apparatus,

causing the information process apparatus to bus-decrypt the bus-encrypted second encrypted key with the session key,

causing the information process apparatus to decrypt the second encrypted key with the first encrypted key,

causing the information process apparatus to bus-decrypt the bus-encrypted third encrypted key with the session key,

causing the information process apparatus to decrypt the third encrypted key with the second encrypted key,

causing the information process apparatus to encrypt the content information transferred to the record and reproduction apparatus with the third encryption, and

causing the information process apparatus to bus-encrypt the encrypted content information with the session key and send the bus-encrypted content information to the record and reproduction apparatus.

47. A program of a record method of a record and

reproduction apparatus that reads information from a record medium and records information thereto and an information process apparatus to which the record and reproduction apparatus is connected through transfer step, content information being encrypted according to a content information encryption method using a first encrypted key managed by a management mechanism, a second encrypted key unique to the record medium, and a third encrypted key generated whenever information is recorded, the content information being recorded to the record medium, the record method comprising the steps of:

causing the record and reproduction apparatus to store the first encrypted key,

causing the record and reproduction apparatus to reproduce the second encrypted key encrypted and recorded on the record medium and decrypt the second encrypted key with the first encrypted key,

causing the record and reproduction apparatus to generate the third encrypted key,

causing the record and reproduction apparatus to encrypt the third encrypted key with the decrypted second encrypted key,

causing the record and reproduction apparatus to authenticate the information process apparatus and generate a session key when the record and reproduction apparatus has successfully authenticated the

information process apparatus,

causing the record and reproduction apparatus to bus-decrypt the bus-encrypted content information supplied from the information process apparatus,

causing the record and reproduction apparatus to encrypt the content information with the third encrypted key,

causing the record and reproduction apparatus to record the third encrypted key and the encrypted content information to the record medium, and

causing the information process apparatus to authenticate the record and reproduction apparatus and generate the session key when the information process apparatus has successfully authenticated the record and reproduction apparatus, and

causing the information process apparatus to bus-encrypt content information transferred to the record and reproduction apparatus with the session key and send the bus-encrypted content information to the record and reproduction apparatus.

48. A program of a record method of a record and reproduction apparatus that reads information from a record medium and records information thereto and an information process apparatus to which the record and reproduction apparatus is connected through transfer step, content information being encrypted according to a content information encryption method using a first

encrypted key managed by a management mechanism, a second encrypted key unique to the record medium, and a third encrypted key generated whenever information is recorded, the content information being recorded to the record medium, the record method comprising the steps of:

causing the record and reproduction apparatus to store the first encrypted key,

causing the record and reproduction apparatus to generate the second encrypted key,

causing the record and reproduction apparatus to encrypt the generated second encrypted key with the first encrypted key,

causing the record and reproduction apparatus to generate the third encrypted key,

causing the record and reproduction apparatus to encrypt the third encrypted key with the generated second encrypted key,

causing the record and reproduction apparatus to authenticate the information process apparatus and generate a session key when the record and reproduction apparatus has successfully authenticated the information process apparatus,

causing the record and reproduction apparatus to bus-decrypt the bus-encrypted content information supplied from the information process apparatus,

causing the record and reproduction apparatus

to encrypt the content information with the third encrypted key,

causing the record and reproduction apparatus to record the second encrypted key, the third encrypted key, and the encrypted content information to the record medium,

causing the information process apparatus to authenticate the record and reproduction apparatus and generate the session key when the information process apparatus has successfully authenticated the record and reproduction apparatus, and

causing the information process apparatus to bus-encrypt content information with the session key and send the bus-encrypted content information to the record and reproduction apparatus.

49. A record medium on which a program of a record method of a record and reproduction apparatus and an information process apparatus is recorded, the record and reproduction apparatus reading information from a record medium and records information thereto and the information process apparatus being connected to the record and reproduction apparatus through transfer step, content information being encrypted according to a content information encryption method using a first encrypted key managed by a management mechanism, a second encrypted key unique to the record medium, and a third encrypted key generated whenever

information is recorded, the content information being recorded to the record medium, the record method comprising the steps of:

causing the record and reproduction apparatus to store the first encrypted key,

causing the record and reproduction apparatus to reproduce the second encrypted key encrypted and recorded on the record medium and decrypt the second encrypted key with the first encrypted key,

causing the record and reproduction apparatus to generate the third encrypted key,

causing the record and reproduction apparatus to encrypt the third encrypted key with the decrypted second encrypted key,

causing the record and reproduction apparatus to authenticate the information process apparatus and generate a session key when the record and reproduction apparatus has successfully authenticated the information process apparatus ,

causing the record and reproduction apparatus to bus-encrypt the second encrypted key that has been encrypted and recorded on the record medium with the session key and transfer the bus-encrypted second encrypted key to the information process apparatus,

causing the record and reproduction apparatus to bus-encrypt the third encrypted key with the session key and transfer the bus-encrypted third encrypted key

to the information process apparatus,

causing the record and reproduction apparatus to bus-decrypt the encrypted and bus-encrypted content information supplied from the information process apparatus,

causing the record and reproduction apparatus to record the third encrypted key and the encrypted content information to the record medium,

causing the information process apparatus to store the first encrypted key,

causing the information process apparatus to authenticate the record and reproduction apparatus and generate the session key when the information process apparatus has successfully authenticated the record and reproduction apparatus,

causing the information process apparatus to bus-decrypt the bus-encrypted second encrypted key with the session key,

causing the information process apparatus to decrypt the second encrypted key with the first encrypted key,

causing the information process apparatus to bus-decrypt the bus-encrypted third encrypted key with the session key,

causing the information process apparatus to decrypt the third encrypted key with the second encrypted key,

causing the information process apparatus to encrypt the content information transferred to the record and reproduction apparatus with the third encryption, and

causing the information process apparatus to bus-encrypt the encrypted content information with the session key and send the bus-encrypted content information to the record and reproduction apparatus.

50. A record medium on which a program of a record method of a record and reproduction apparatus and an information process apparatus is recorded, the record and reproduction apparatus reading information from a record medium and records information thereto and the information process apparatus being connected to the record and reproduction apparatus through transfer step, content information being encrypted according to a content information encryption method using a first encrypted key managed by a management mechanism, a second encrypted key unique to the record medium, and a third encrypted key generated whenever information is recorded, the content information being recorded to the record medium, the record method comprising the steps of:

causing the record and reproduction apparatus to store the first encrypted key,

causing the record and reproduction apparatus to generate the second encrypted key,

causing the record and reproduction apparatus to encrypt the generated second encrypted key with the first encrypted key,

causing the record and reproduction apparatus to generate the third encrypted key,

causing the record and reproduction apparatus to encrypt the third encrypted key with the generated second encrypted key,

causing the record and reproduction apparatus to authenticate the information process apparatus and generate a session key when the record and reproduction apparatus has successfully authenticated the information process apparatus,

causing the record and reproduction apparatus to bus-encrypt the second encrypted key with the session key and transfers the bus-encrypted second encrypted key to the information process apparatus,

causing the record and reproduction apparatus to bus-encrypt the third encrypted key with the session key and transfer the bus-encrypted third encrypted key to the information process apparatus,

causing the record and reproduction apparatus to bus-decrypt the encrypted and bus-encrypted content information supplied from the information process apparatus, and

causing the record and reproduction apparatus to record the second encrypted key, the third encrypted

key, and the encrypted content information to the record medium, and

causing the information process apparatus to store the first encrypted key,

causing the information process apparatus to authenticate the record and reproduction apparatus and generate the session key when the information process apparatus has successfully authenticated the record and reproduction apparatus,

causing the information process apparatus to bus-decrypt the bus-encrypted second encrypted key with the session key,

causing the information process apparatus to decrypt the second encrypted key with the first encrypted key,

causing the information process apparatus to bus-decrypt the bus-encrypted third encrypted key with the session key,

causing the information process apparatus to decrypt the third encrypted key with the second encrypted key,

causing the information process apparatus to encrypt the content information transferred to the record and reproduction apparatus with the third encryption, and

causing the information process apparatus to bus-encrypt the encrypted content information with the

session key and send the bus-encrypted content information to the record and reproduction apparatus.

51. A record medium on which a program of a record method of a record and reproduction apparatus and an information process apparatus is recorded, the record and reproduction apparatus reading information from a record medium and records information thereto and the information process apparatus being connected to the record and reproduction apparatus through transfer step, content information being encrypted according to a content information encryption method using a first encrypted key managed by a management mechanism, a second encrypted key unique to the record medium, and a third encrypted key generated whenever information is recorded, the content information being recorded to the record medium, the record method comprising the steps of:

causing the record and reproduction apparatus to store the first encrypted key,

causing the record and reproduction apparatus to reproduce the second encrypted key encrypted and recorded on the record medium and decrypt the second encrypted key with the first encrypted key,

causing the record and reproduction apparatus to generate the third encrypted key,

causing the record and reproduction apparatus to encrypt the third encrypted key with the decrypted

second encrypted key,

causing the record and reproduction apparatus to authenticate the information process apparatus and generate a session key when the record and reproduction apparatus has successfully authenticated the information process apparatus,

causing the record and reproduction apparatus to bus-decrypt the bus-encrypted content information supplied from the information process apparatus,

causing the record and reproduction apparatus to encrypt the content information with the third encrypted key,

causing the record and reproduction apparatus to record the third encrypted key and the encrypted content information to the record medium, and

causing the information process apparatus to authenticate the record and reproduction apparatus and generate the session key when the information process apparatus has successfully authenticated the record and reproduction apparatus, and

causing the information process apparatus to bus-encrypt content information transferred to the record and reproduction apparatus with the session key and send the bus-encrypted content information to the record and reproduction apparatus.

52. A record medium on which a program of a record method of a record and reproduction apparatus

and an information process apparatus is recorded, the record and reproduction apparatus reading information from a record medium and records information thereto and the information process apparatus being connected to the record and reproduction apparatus through transfer step, content information being encrypted according to a content information encryption method using a first encrypted key managed by a management mechanism, a second encrypted key unique to the record medium, and a third encrypted key generated whenever information is recorded, the content information being recorded to the record medium, the record method comprising the steps of:

causing the record and reproduction apparatus to store the first encrypted key,

causing the record and reproduction apparatus to generate the second encrypted key,

causing the record and reproduction apparatus to encrypt the generated second encrypted key with the first encrypted key,

causing the record and reproduction apparatus to generate the third encrypted key,

causing the record and reproduction apparatus to encrypt the third encrypted key with the generated second encrypted key,

causing the record and reproduction apparatus to authenticate the information process apparatus and

generate a session key when the record and reproduction apparatus has successfully authenticated the information process apparatus,

causing the record and reproduction apparatus to bus-decrypt the bus-encrypted content information supplied from the information process apparatus,

causing the record and reproduction apparatus to encrypt the content information with the third encrypted key,

causing the record and reproduction apparatus to record the second encrypted key, the third encrypted key, and the encrypted content information to the record medium,

causing the information process apparatus to authenticate the record and reproduction apparatus and generate the session key when the information process apparatus has successfully authenticated the record and reproduction apparatus, and

causing the information process apparatus to bus-encrypt content information with the session key and send the bus-encrypted content information to the record and reproduction apparatus.